

REMARKS

This Response supplements the Response to Office Action filed January 5, 2005; and further amends the claims in order to expedite prosecution in a manner that is believed to place the case in condition for allowance. Comments and remarks set forth in the Response to Office Action filed January 5, 2005 are incorporated herein by reference for the convenience of the Examiner.

Claims 1-12, 16-22, 26-32 and 36-39 are pending in the present application. Claims 13-15, 23-25 and 33-35 were canceled in the Response to Office Action filed January 5, 2005; claims 1, 5-9, 18, 19, 28, 29, 38 and 39 are cancelled in the present Response; claims 18, 28 and 38 were amended in the Response to Office Action filed January 5, 2005; claims 2-4, 10, 16, 17, 26, 27, 36 and 37 were amended in this Response; and no claims were added. Claim 2 was amended to depend from claim 10, claim 3 was amended to depend from claim 20, claim 4 was amended to depend from claim 30, claim 17 was amended to depend from claim 10, claim 27 was amended to depend from claim 20 and claim 37 was amended to depend from claim 30. Reconsideration of the claims is respectfully requested.

Applicants wish to thank the Examiner for taking the time to participate in a tele-conference on April 7, 2005. During this conference ways of distinguishing the present invention from the prior art, especially in regard to the Serverwatch reference were discussed. This amendments to the claims were made in view of those comments, in order to expedite prosecution and with the goal of placing the claims in condition for immediate allowance.

I. **35 U.S.C. § 103, Obviousness, Claims 1-10, 12, 20, 22, 30 and 32**

The Examiner has rejected claims 1-10, 12, 20, 22, 30 and 32 under 35 U.S.C. § 103 as being unpatentable over Arnold et al (5440723) (hereinafter "Arnold") in view of Serverwatch – Network Associates Ships CyberCop Sting (hereinafter "Serverwatch"). This rejection is respectfully traversed.

As to claims 1-10, 12, 20, 22, 30 and 32, the Office Action states:

With respect to Claim 1, Arnold et al meets the limitation of "a local server" on Fig. 1A; and "a plurality of client data processing systems" on Fig. 1B; and "...broadcasts an indication that a virus attack is

underway to all devices within the network data processing system" on column 2, lines 30-33, column 24, lines 32-42; and "ignores all further access requests by the offending system until receiving an indication that the offending system has been disinfected, and directs the local server to disconnect the offending system from the network data processing system" on column 5, lines 59-65, and on column 24, lines 44-57. Arnold however does not meet the following limitation.

The limitation of "a bait server, wherein the bait server monitors itself and, responsive to an attempt from an offending system within the network data processing system to access the bait server" is met by Serverwatch on pages 1 and 2.

It would have been obvious to combine the teachings of Serverwatch within the system of Arnold et al because the bait server provides a dedicated, convenient and less expensive way of monitoring a large network. A dedicated bait server requires less maintenance than multiple decoy programs/servers and hence simplifies an administrator's job of protecting the network. It is obvious to ignore all further access requests from the offending system until the infected system is uninfected so as not to spread the virus to the rest of the network.

Office Action dated October 5, 2004, page 1.

A fundamental notion of patent law is the concept that invention lies in the new combination of old elements. Therefore, a rule that every invention could be rejected as obvious by merely locating each element of the invention in the prior art and combining the references to formulate an obviousness rejection is inconsistent with the very nature of "invention." Consequently, a rule exists that a combination of references made to establish a *prima facie* case of obviousness must be supported by some teaching, suggestion, or incentive contained in the prior art which would have led one of ordinary skill in the art to make the claimed invention.

The Examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992).

Additionally, in comparing Arnold and Serverwatch to the claimed invention, the claim limitations of the presently claimed invention may not be ignored in an obviousness determination.

The present invention, in independent claim 10, which is representative of claims 20 and 30 with regard to similarly recited subject matter, recites:

10. A method for detecting the presence of a computer virus, the method comprising;
receiving, at a bait server, a request to perform a function on the bait server;
identifying an offending system from which the request originated;
alerting a local server that a virus attack is in progress and of the identity of the offending system; and
disconnecting the offending system from the network.

Arnold does not teach the feature of “disconnecting the offending system from the network.” The Examiner points to column 5, lines 59-65 and column 24, lines 44-57 of Arnold as teaching this feature:

If the anomaly is found to be due to a known virus or some slight alteration of it, the method proceeds to Step B1 where the user is alerted, and the virus removed (killed) by traditional methods, such as restoration from backup (either automatically or manually by the user) or disinfection (removal of the virus from all of the software it has infected.) In general, disinfection is only acceptable if the virus is found to be an exact copy of a known virus. This implies that the system verify the identification made by the virus scanner.

If VIRSCAN (Block 0) has identified one or more infected files, an attempt is made to restore each infected file to an uninfected condition. VERV is capable of removing many of the most common viruses from infected files by determining whether the virus is an exact copy of one that it is capable of removing. If so, VERV removes the virus. If the virus cannot be removed by VERV, an automatic restore from a tape backup or from a read-only directory on a server, or from another machine on the network is attempted. If an automatic restoration of the infected file cannot be accomplished, the user receives a message describing the situation, with instructions for manually restoring the file from backup.

Neither of the above cited passages teaches the feature of “disconnecting the offending system from the network.” The first cited passage, column 5, lines 59-65, teaches that when a virus is found, the user is alerted and an attempt is made to eliminate the virus. The second cited passage, column 24, lines 44-57, teaches that once a virus has

been detected VERV tries to eliminate the virus. If VERV is unsuccessful, then an automatic restoration of backup files is attempted. If that fails, a message is generated and sent to the user, instructing the user to manually restore the files from backup. Neither passage, when read separately or together, teaches the feature of "disconnecting the offending system from the network." Therefore, the proposed combination does not result in the claimed invention. Accordingly, the Examiner has failed to state a *prima facie* case of obviousness.

Furthermore, nowhere does Arnold teach or suggest the feature of "disconnecting the offending system from the network." Arnold describes a process whereby, when a virus is detected, other computers are notified. Arnold teaches that this signal, the kill signal, merely contains information and is intended primarily to inform neighboring computers of an anomaly existing and secondarily to induce them to begin their own virus protection routines, as explained in a passage in column 19, line 58 through column 20, line 11:

The kill signal may take a variety of forms and provide as little or as much information as is appropriate or practical. For example, in one embodiment the infected computer simply sends an "I'm infected" signal (one bit of information) to its neighbor(s) whenever it enters Step B (Scan for Known Viruses), thereby inducing all of the neighbors to also enter Step B themselves. In another embodiment, the infected computer sends an "I'm infected" signal after it has cleaned itself up (completed Step B successfully), and also sends the name of the virus (if it was previously known) and its signature(s), whether the virus was previously known or not. The signature(s) may have been determined in Step E. In a further embodiment, the infected computer sends an "I'm infected" signal when it enters Step C, i.e., after it fails to identify the anomaly as a known virus, thereby inducing its neighbors to enter Steps B and C. Other strategies may also be used, other than those specifically detailed above. In all cases, the end result is that other computers on the network are alerted to the presence of an anomaly, which may be a known or an unknown virus, within the network.

Thus, nowhere does Arnold teach or suggest the feature of "disconnecting the offending system from the network." Therefore, the proposed combination does not result in the claimed invention. Accordingly, the Examiner has failed to state a *prima facie* case of obviousness.

Furthermore, Serverwatch does not cure the deficiencies of Arnold. Serverwatch does not teach the features missing from Arnold, including "disconnecting the offending system from the network," nor does the Examiner cite any portion of Serverwatch that teaches these features. Therefore, the proposed combination does not result in the claimed invention. Accordingly, the Examiner has failed to state a *prima facie* case of obviousness.

Additionally, the present invention is directed at detecting viruses and worms on a computer or computer network and preventing their spread. Serverwatch does not teach the problem or its source. Instead, Serverwatch is directed towards detecting and tracking unauthorized users, or computer hackers. That is the Serverwatch reference discuss a product that "silently traces and tracks hackers, recording and reporting all intrusive activity to security administrators." (See Serverwatch, page 1). Therefore, one of ordinary skill in the art would not be motivated to combine or modify the references in the manner required to form the solution disclosed in the claimed invention.

Therefore, for all the reasons stated above, Applicants believe that the cited references do not teach all the features of independent claims 10, 20 and 30. Therefore, the proposed combination does not result in the claimed invention. Accordingly, the Examiner has failed to state a *prima facie* case of obviousness. Accordingly, Applicants respectfully submit that claims 10, 20 and 30 are patentable over the Arnold and Serverwatch references.

Claims 2-4, 12, 17, 22, 27, 32 and 37 are dependent claims that depend from independent claims 10, 20 and 30. As Applicants have already demonstrated that independent claims 10, 20 and 30 are patentable over the Arnold and Serverwatch references, Applicants submit that dependent claims 2-4, 12, 17, 22, 27, 32 and 37 are patentable over the Arnold and Serverwatch references at least by virtue of depending from an allowable claim. Consequently, Applicants respectfully submit that the rejection of claims 2-4, 12, 17, 22, 27, 32 and 37 have been overcome. Additionally, several claims recite other additional combinations of features not suggested by the Arnold and Serverwatch references.

For example, regarding claims 2, 3 and 4, the Examiner concedes, and Applicants agree, that Arnold does not teach the feature of "not publishing the bait server's address

to the network..” However, Serverwatch does not teach this feature either. The Examiner points to page 1 of Serverwatch as teaching this feature. The Examiner has stated that “[t]his is because the decoy server creates a fictitious presence within the network.” However, just because the Serverwatch product creates a fictitious presence, it does not follow that the address of the server is “not published to the plurality of client data processing systems.” What the Serverwatch advertisement states is:

Network Associates, Inc. today announced the availability of its CyberCop Sting software, a new “decoy” server that silently traces and tracks hackers, recording and reporting all intrusive activity to security administrators. CyberCop Sting is a component of the CyberCop intrusion protection software family which also includes CyberCop Monitor, a real-time intrusion detection application that monitors critical systems and networks for signs of attack and CyberCop Scanner, a network vulnerability scanner.

CyberCop Sting allows IS managers to silently monitor suspicious activity on their corporate network and identify potential problems. It operates by creating a series of fictitious corporate systems on a specially outfitted server that combines moderate security protection with sophisticated monitoring technology. The Sting product creates a decoy, virtual TCP/IP network on a single server or workstation and can simulate a network containing several different types of network devices, including Windows NT servers, Unix servers and routers. Each virtual network device has a real IP address and can receive and send genuine-looking packets from and to the larger network environment. Each virtual network node can also run simulated daemons, such as finger and FTP, to further emulate the activity of a genuine system and avoid suspicion by would-be intruders. While watching all traffic destined to hosts in its virtual network, Sting performs IP fragmentation reassembly and TCP stream reassembly on the packets destined to these hosts, convincing snoopers of the legitimacy of the secret network they've discovered.

CyberCop Sting provides a number of benefits for security administrators, including:

- Detection of suspicious activity inside network; Log files serve to alert administrators to potential attackers prying into reserved areas.
- Virtual decoy network can contain multiple “hosts” without the expense and maintenance that real systems require.
- CyberCop Sting software's virtual hosts return realistic packet information.

- CyberCop Sting logs snooper activity immediately, so collection of information about potential attackers can occur before they leave.
- CyberCop Sting requires very little file space but creates a sophisticated virtual network.

Network Associates' CyberCop Intrusion Protection suite is a collection of integrated security tools developed to provide network risk assessment scanning (Scanner), real-time intrusion monitoring (Monitor) and decoy trace-and-track capabilities (Sting) to enhance the security and survivability of enterprise networks and systems. The suite also includes features such as AutoUpdate, modular construction, and Active Security integration to provide product integrity. A Network Associates white paper on next-generation intrusion detection is available at <http://www.nai.com/activesecurity/files/ids.doc>.

The above cited passages teach that the Serverwatch product creates a series of fictitious systems on a special server. However, nowhere does the advertisement state that the address of the special server is "not published to the plurality of client data processing systems." Simply creating a virtual device does not mean that the address of the device, or the server on which the virtual device resides, is unknown to other, real servers and devices. It just means that the device is not a real, physical device. Thus, nowhere does Serverwatch teach or suggest the feature of "wherein the address of the bait server is not published to the plurality of client data processing systems." Therefore, the proposed combination does not result in the claimed invention. Accordingly, the Examiner has failed to state a *prima facie* case of obviousness.

Claims 12, 22 and 32 recite the features of "receiving a reconnect request from the offending system" and "reconnecting the offending system to the network." Neither Arnold nor Serverwatch teach or suggest these features. The Examiner points to column 24, lines 61-65 as teaching these features:

The resulting disinfected file is then checked by running CHECKUP (Block B) and determining whether the checksum of the file matches the value it had prior to infection. If not, automatic or manual restoration of the original file can be attempted.

The above cited passage teaches verifying that the disinfected file has indeed been disinfected. The Examiner further states that "it is inherent that the computer is

reconnected to the network after the disinfection is verified.” However, as was discussed above in regards to claim 10, Arnold does not teach disconnecting an infected computer from the network. Therefore, it follows that if Arnold does not teach disconnecting the infected system, Arnold cannot teach receiving a request to reconnect the computer once it has been disinfected or reconnecting the computer once it has been disinfected. Thus, Arnold does not teach the features of “receiving a reconnect request from the offending system” or “reconnecting the offending system to the network.” Therefore, the proposed combination does not result in the claimed invention. Accordingly, the Examiner has failed to state a *prima facie* case of obviousness.

Additionally, claims 17, 27 and 37 recite the feature of “instructing all devices within the network to ignore all requests from the offending system until the offending system has been disinfected and is available for network communication.” Arnold does not teach or suggest this feature. The Examiner points to column 5, lines 59-65 and column 24, lines 44-57 of Arnold, cited above, as teaching this feature. As was discussed above, the first cited passage teaches that when a virus is found, the user is alerted and an attempt is made to eliminate the virus. The second cited passage teaches that once a virus has been detected VERV tries to eliminate the virus. If VERV is unsuccessful, then an automatic restoration of backup files is attempted. If that fails, a message is generated and sent to the user, instructing the user to manually restore the files from backup. Neither passage, when read separately or together, teaches the feature of “instructing all devices within the network to ignore all requests from the offending system until the offending system has been disinfected and is available for network communication.” Therefore, the proposed combination does not result in the claimed invention. Accordingly, the Examiner has failed to state a *prima facie* case of obviousness.

Furthermore, nowhere does Arnold teach the feature of “instructing all devices within the network to ignore all requests from the offending system until the offending system has been disinfected and is available for network communication.” Instead, as can be seen in the above cited passage, column 19, line 58 through column 20, line 11, Arnold teaches that the infected system can continue interacting with the rest of the network as shown by several embodiments in which the infected computer sends information to other computers prior to the infected computer’s being cleaned of the

virus. Thus, nowhere does Arnold teach or suggest the feature of “instructing all devices within the network to ignore all requests from the offending system until the offending system has been disinfected and is available for network communication.” Therefore, the proposed combination does not result in the claimed invention. Accordingly, the Examiner has failed to state a *prima facie* case of obviousness.

Furthermore, Serverwatch does not cure the deficiencies of Arnold. Serverwatch does not teach the features missing from Arnold, including “instructing all devices within the network to ignore all requests from the offending system until the offending system has been disinfected and is available for network communication,” nor does the Examiner cite any portion of Serverwatch that teaches these features. Therefore, the proposed combination does not result in the claimed invention. Accordingly, the Examiner has failed to state a *prima facie* case of obviousness.

Therefore, the rejection of claims 1-10, 12, 20, 22, 30 and 32 under 35 U.S.C. § 103 has been overcome.

II. 35 U.S.C. § 103, Obviousness, Claims 11, 21 and 31

The Examiner has rejected claims 11, 21 and 31 under 35 U.S.C. § 103 as being unpatentable over Arnold et al (5440723) in view of Serverwatch – Network Associates Ships CyberCop Sting in further view of Kim et al (6701440 B1). This rejection is respectfully traversed.

As to claims 11, 21, 31, the Office Action states:

With respect to Claim 11, all the limitation is met by the combination of Arnold et al and Serverwatch except for the following limitation. The limitation of “prior to disconnecting the offending system, notifying the offending system that it is infected with a virus” is met by Kim et al on column 3, lines 45-47 and 54-61.

It would have been obvious to one of ordinary skill in the art to combine the teachings of Kim et al within the combination of Arnold et al and Serverwatch because quarantining the infected machine and then notifying it that it has been infected prevents further spread of the virus to the rest of the network.

Office Action dated October 5, 2004, page 4.

The Arnold reference does not teach or suggest all the claim limitations in claims 11, 21 and 31, as argued in the response to the rejection of claim 10 above.

Furthermore, as argued in the response to the rejection of claim 10 above, Serverwatch does not cure the deficiencies in Arnold.

Additionally, Kim does not cure the deficiencies of Arnold and Serverwatch. Kim does not teach the features missing from Arnold and Serverwatch, including "instructing all devices within the network to ignore all requests from the offending system until the offending system has been disinfected and is available for network communication," and "disconnecting the offending system from the network," nor does the Examiner cite any portion of Kim that teaches these features.

Thus, claims 11, 21 and 31 are patentable over the cited references because the combination of the Arnold reference with Serverwatch and Kim would not reach the presently claimed invention. The features relied upon as being taught in the Arnold reference are not taught or suggested by that reference, as explained above. Neither Serverwatch nor Kim cures the deficiencies of Arnold. As a result, a combination of these references would not reach the claimed invention in claims 11, 21 and 31.

In view of the above, Applicants submit that dependent claims 11, 21 and 31 are not taught or suggested by Arnold, Serverwatch, Kim or any combination thereof. Claims 11, 21 and 31 are dependent claims depending on independent claims 10, 20 and 30. Applicants have already demonstrated claims 10, 20 and 30 to be in condition for allowance. Applicants respectfully submit that claims 11, 21 and 31 are also allowable, at least by virtue of their dependency on allowable claims.

Therefore, the rejection of claims 11, 21, 31 under 35 U.S.C. § 103 has been overcome.

III. 35 U.S.C. § 103, Obviousness, Claims 16-19, 26-29 and 36-39

The Examiner has rejected claims 16-19, 26-29, and 36-39 under 35 U.S.C. § 103 as being unpatentable over Arnold et al (5440723). This rejection is respectfully traversed. Claims 16, 26 and 36 have been substantially modified in order expedite prosecution in an effort to put the claims in condition for immediate allowance.

As to claims 16-19, 26-29, 36-39, the Office Action states:

With respect to Claim 16, Arnold et al meets the limitation of “monitoring a network for the presence of a computer virus” on column 2, lines 51-55; and “responsive to a determination that a virus is detected, determining the identify of an offending system within the network from which the virus entered the network” on column 4, lines 61-66; and “directing the local server to disconnect the offending system from the network” on column 19, lines 60-68, and on column 20, lines 1-3.

It would have been obvious to one of ordinary skill in the art at the time of the invention to disconnect the infected computers from the network before the systems are cleaned up so as to prevent further spread of the virus. The “I’m infected” message sent by the infected system(s) has its identifying information as part of the message sent or else the recipient of this message would not know which computer in the network had sent this message and was infected.

Office Action dated October 5, 2004, page 6-7.

Independent claim 16, which is representative of independent claims 26 and 36 with regard to similarly recited subject matter, recites:

16. A method in a bait server for detecting the presence of a computer virus, the method comprising:
not publishing the bait server’s address to a network;
monitoring the network for the presence of a computer virus;
responsive to a determination that a virus is detected, determining the identity of an offending system within the network from which the virus entered the network; ~~and~~
notifying a local server of the presence of the virus and the identity of the offending system;
instructing all devices within the network to ignore all requests from the offending system until the offending system has been disinfected and is available for network communication;
directing the local server to disconnect the offending system from the network; and
responsive to an indication that the offending system has been disinfected and responsive to a reconnect request from the offending system to the local server, reconnecting the offending system to the network.

The Arnold reference does not teach or suggest all the claim limitations in claim 16. Specifically, Arnold does not teach feature of “instructing all devices within the

network to ignore all requests from the offending system until the offending system has been disinfected and is available for network communication.” Arnold does not teach this feature. The Examiner points to column 19, line 60 through column 20, line 11, reproduced above, as teaching this feature. However, the above cited passage does not teach this feature. As was discussed above in the response to the rejection of claim 17, Arnold does not teach or suggest the feature of “instructing all devices within the network to ignore all requests from the offending system until the offending system has been disinfected and is available for network communication.” Therefore, even in view of the Examiner’s comments, Arnold would not teach or suggest the presently claimed invention. Accordingly, the Examiner has failed to state a *prima facie* case of obviousness.

Additionally, Arnold does not teach the feature of “directing the local server to disconnect the offending system from the network.” The Examiner points to column 19, line 60 through column 20, line 3, reproduced above, as teaching this feature. However, as was discussed above in the response to the rejection of claim 10, Arnold does not teach the feature of disconnecting an offending or infected system from the network. Therefore, it follows that Arnold does not teach the feature of “directing the local server to disconnect the offending system from the network.” Therefore, even in view of the Examiner’s comments, Arnold would not teach or suggest the presently claimed invention. Accordingly, the Examiner has failed to state a *prima facie* case of obviousness.

Furthermore, As was discussed above regarding claims 2-4, Arnold does not teach the feature of “not publishing the bait server’s address to a network.” Therefore, even in view of the Examiner’s comments, Arnold would not teach or suggest the presently claimed invention. Accordingly, the Examiner has failed to state a *prima facie* case of obviousness.

Additionally, claim 16 recites the feature of “responsive to an indication that the offending system has been disinfected and responsive to a reconnect request from the offending system, reconnecting the offending system to the network.” Arnold does not teach this feature. The Examiner points to column 24, lines 61 through 65, reproduced above, as teaching this feature. However, the above cited passage does not teach this

feature. As was discussed above in the response to the rejection of claim 12, Arnold does not teach or suggest "receiving a reconnect request from the offending system" or "reconnecting the offending system to the network." Therefore, it follows for the same reasons, that Arnold does not teach the feature of "responsive to an indication that the offending system has been disinfected and responsive to a reconnect request from the offending system, reconnecting the offending system to the network," as recited in claim 16 of the present invention. Thus, Arnold does not teach each and every element of claim 16. Therefore, even in view of the Examiner's comments, Arnold would not teach or suggest the presently claimed invention. Accordingly, the Examiner has failed to state a *prima facie* case of obviousness.

Therefore, for all the reasons stated above, Applicants believe that Arnold does not teach all the features of independent claims 16, 26 and 36. Additionally, for all the reasons stated above, Applicants believe that neither Arnold nor the Examiner's comments teach all the features of independent claims 16, 26 and 36. Therefore, even in view of the Examiner's comments, Arnold would not teach or suggest the claimed invention. Accordingly, the Examiner has failed to state a *prima facie* case of obviousness. Therefore, Applicants respectfully submit that claims 16, 26 and 36 are patentable over Arnold.

Therefore, the rejection of claims 16-19, 26-29, and 36-39 under 35 U.S.C. § 102 and 35 U.S.C. § 103 has been overcome.

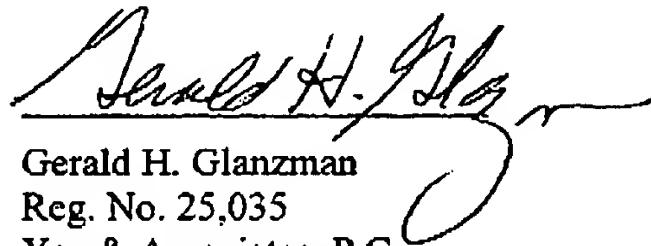
IV. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance.

The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: April 13, 2005

Respectfully submitted,



Gerald H. Glanzman
Reg. No. 25,035
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants

GHG/bj